3rd Conference on Banking Development, Stability, and Sustainability

Carlos Arena, R3

Quick Introduction to Blockchain and Distributed Ledger Technology

In the beginning…

Cryptocurrency

Blockchain

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

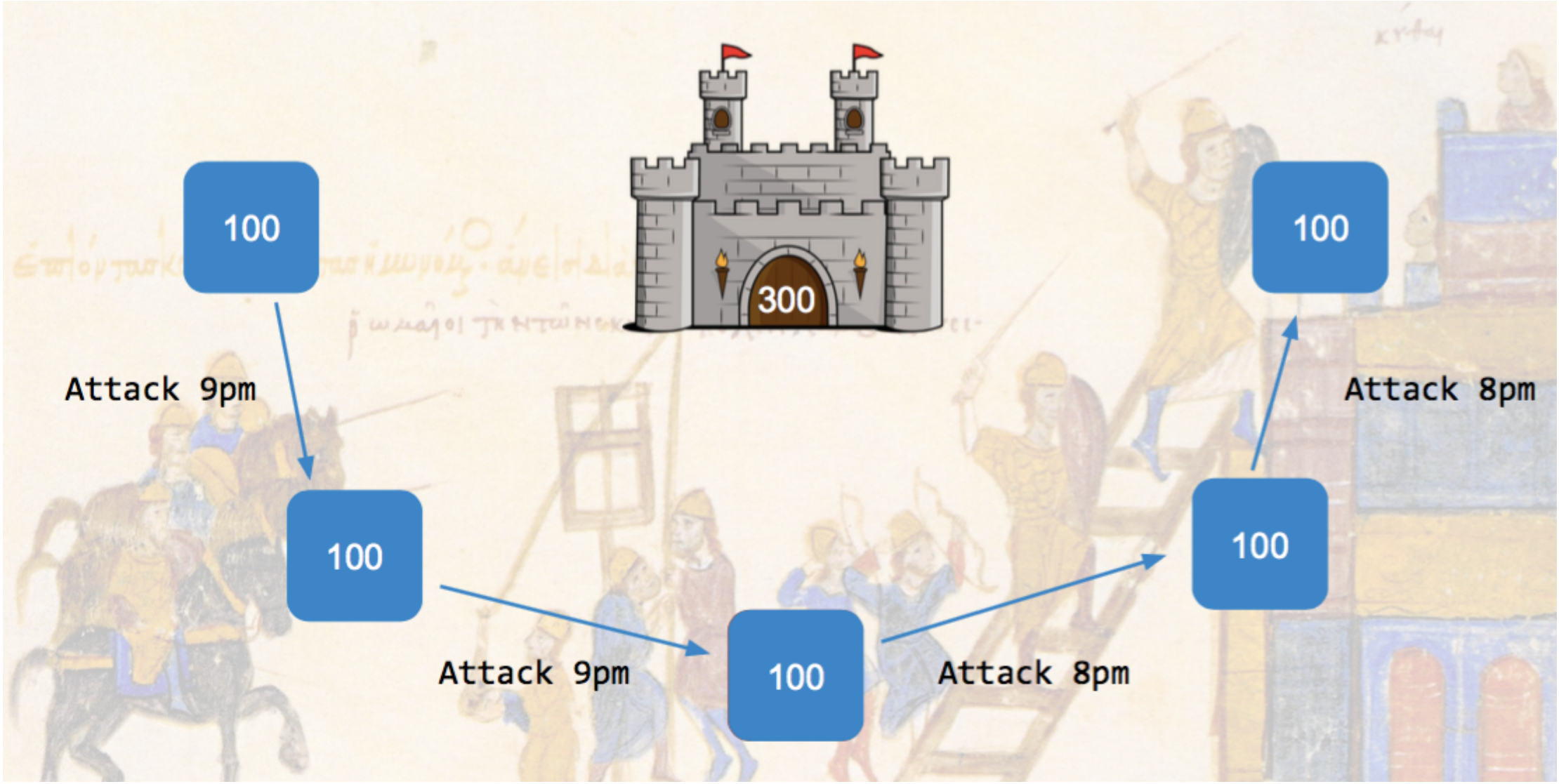
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing

Proof-of-work

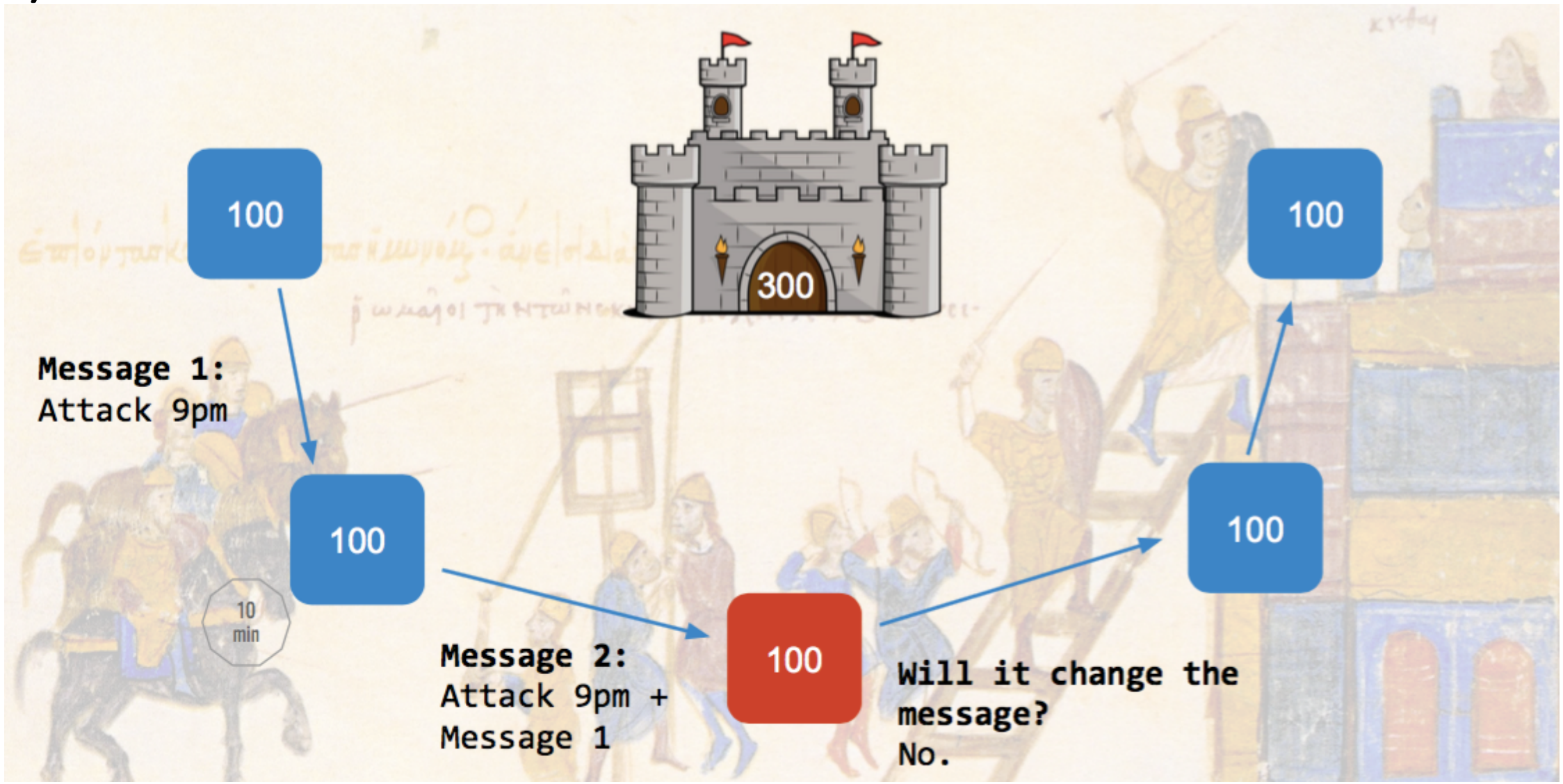
Mining

1. Byzantine General Problem

1. Byzantine General Problem



1. Byzantine General Problem

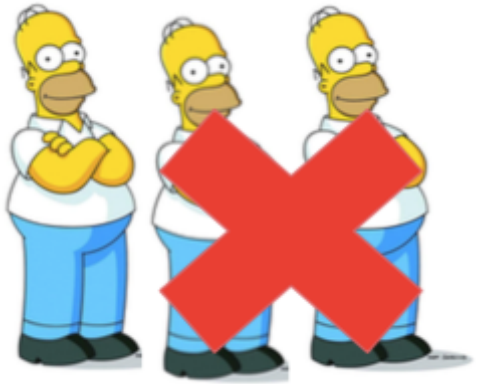


2. Double Spend

Blockchain = Source of Truth

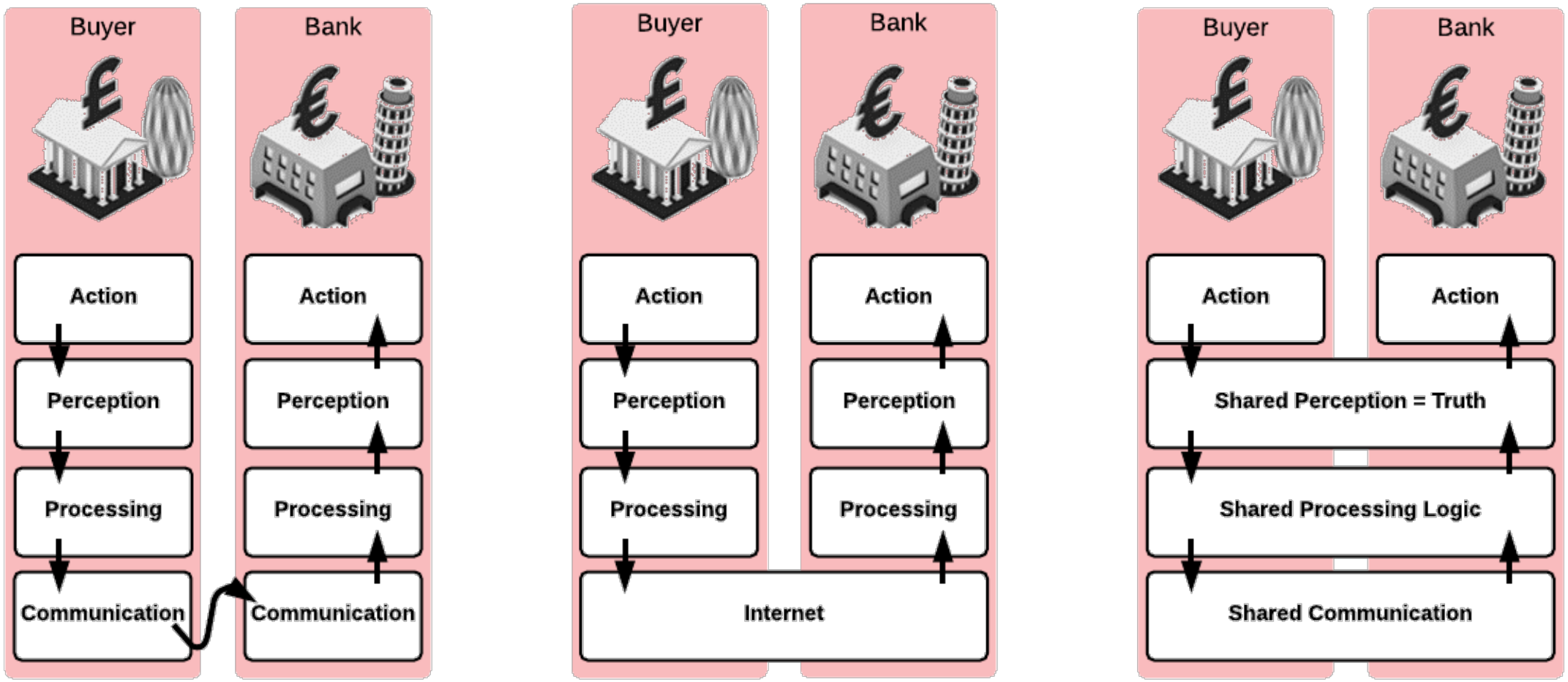
1) Byzantine General Problem

2) Double Spend



Source of Truth

The Significant Evolutionary Step of DLT.



Application of DLT to Finance

What makes cash interesting?

What makes cash interesting?

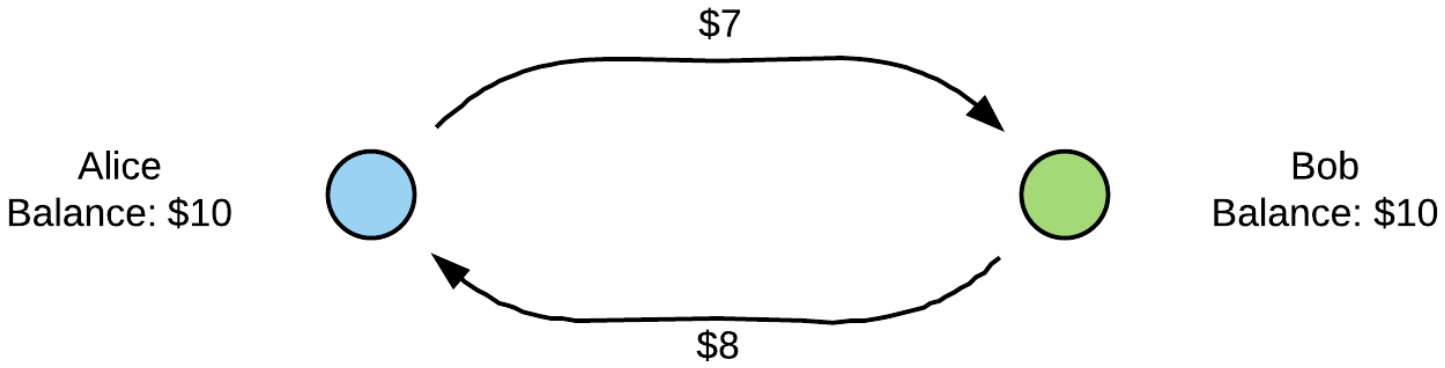
- It’s a building block for many (most?) financial applications
- It’s fungible
- It can be exchanged it for other assets
- It can be used to make promises
- It can be settled now or in the future (gross vs. deferred net settlement)

Deferred Net Settlement

Liquidity Savings Mechanisms

A Simple Example

Alice owes Bob $7, but doesn't want to pay yet (might need $5 for something more urgent later)

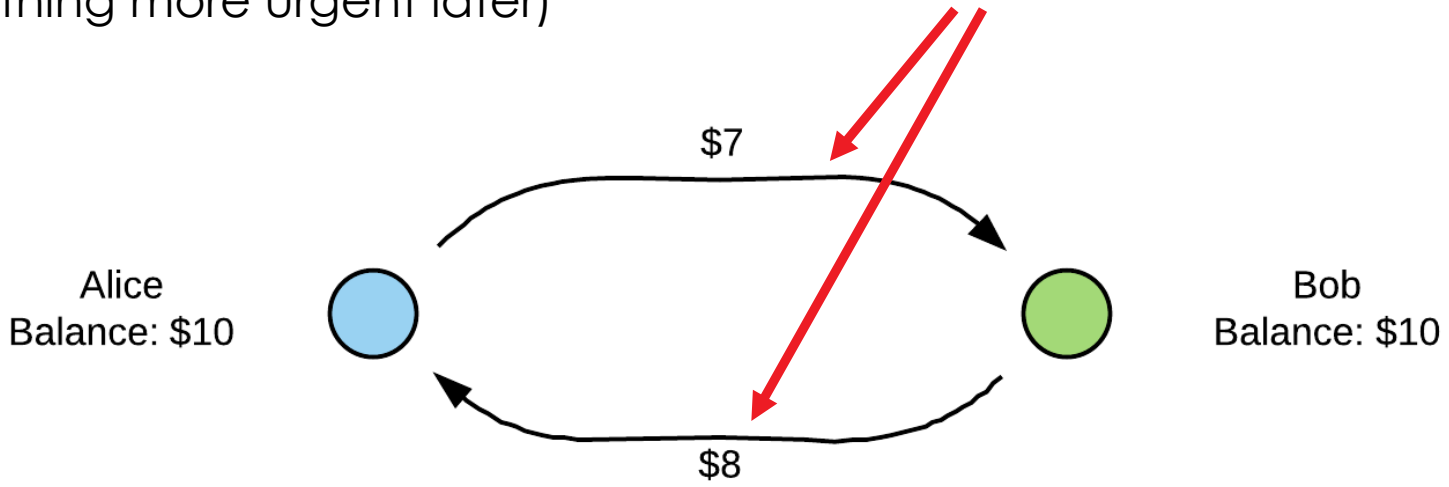


Bob owes Alice $8, but doesn't want to pay yet (might need $6 for something more urgent later)

A Simple Example

Alice owes Bob $7, but doesn't want to pay yet (might need $5 for something more urgent later)

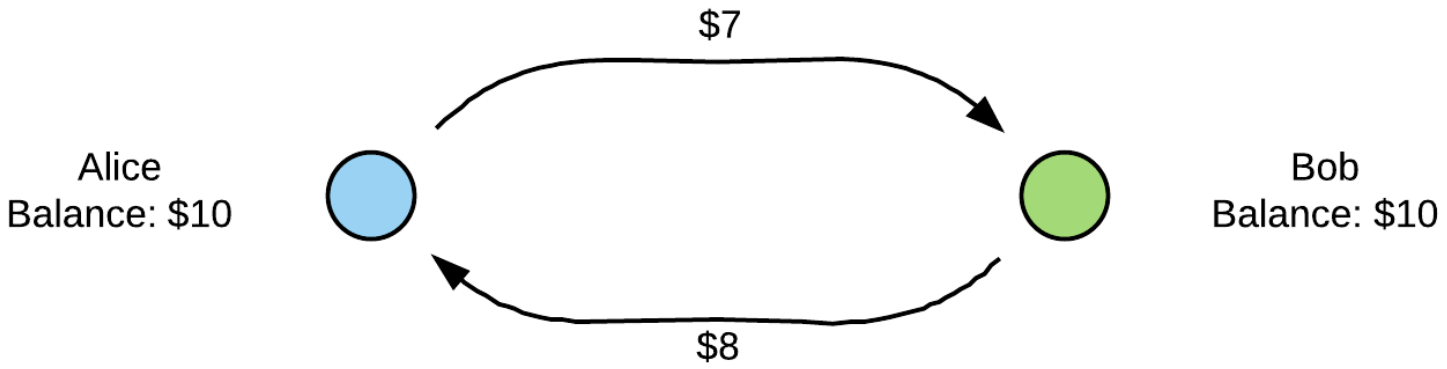
Promises to pay, not actual payments!



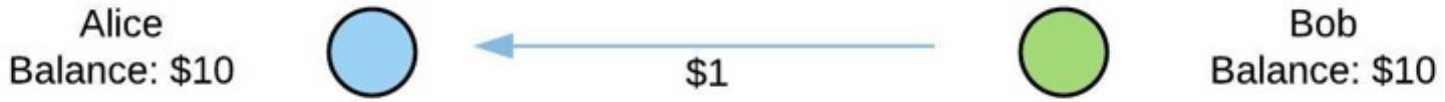
Bob owes Alice $8, but doesn't want to pay yet (might need $6 for something more urgent later)

A Simple Example

We can't just create a transaction with both payments because in other scenarios the balances may not be sufficient (e.g. if the starting balances were both $5), and we can't pay using states that we don't yet have

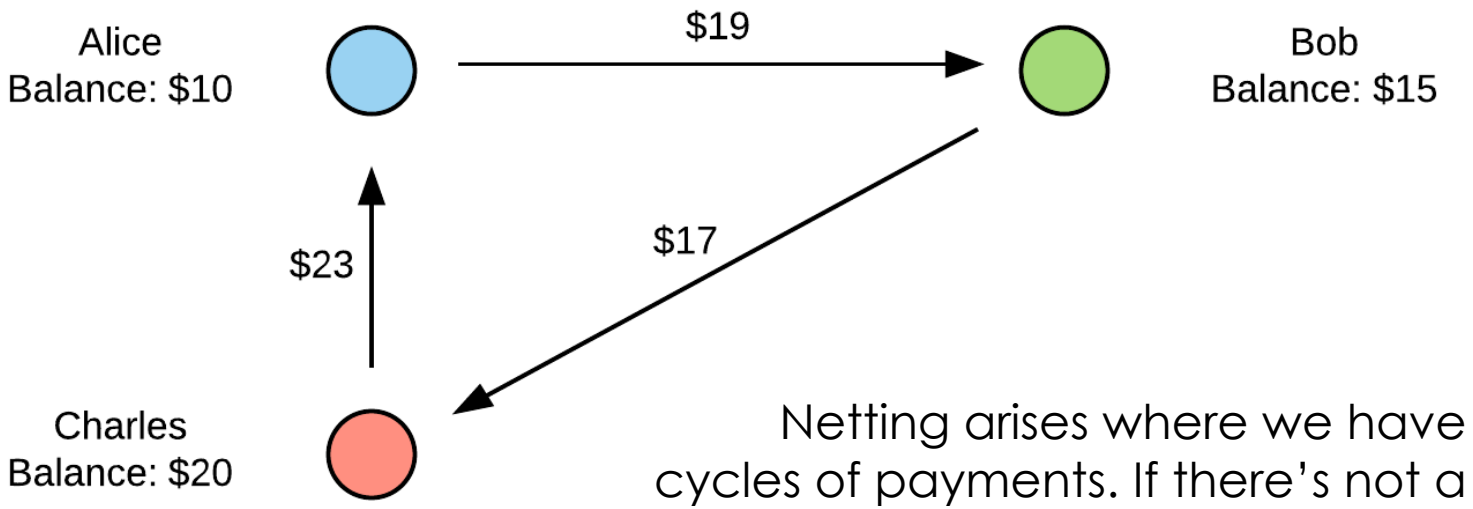


A Simple Example Resolved



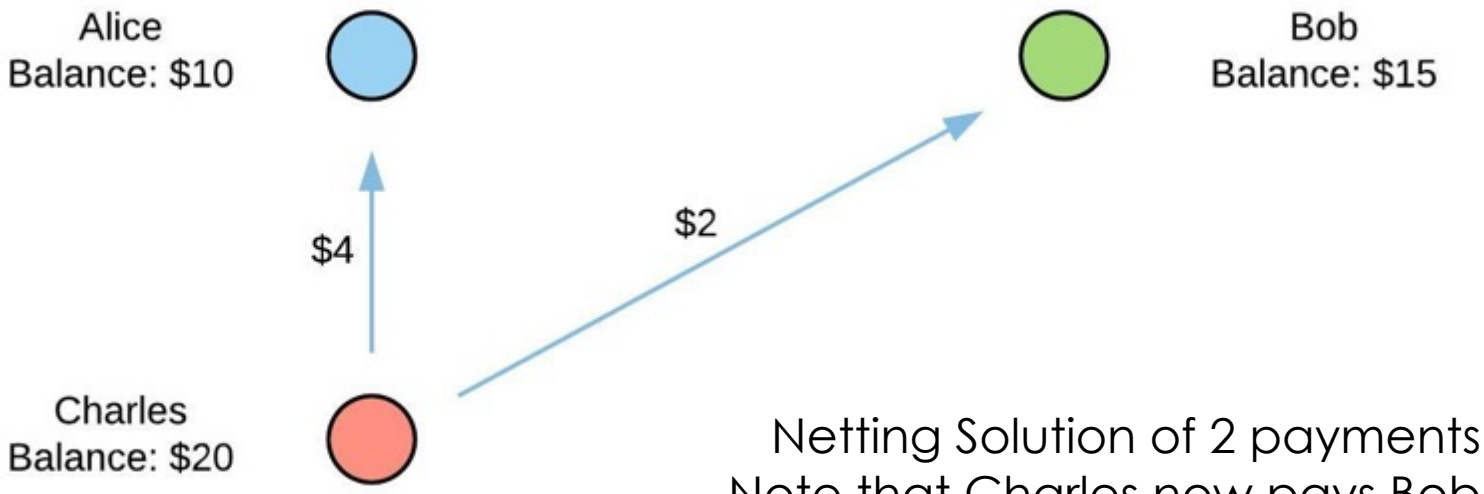
Net settlement of $1 will leave both happy

A More Tricky Example



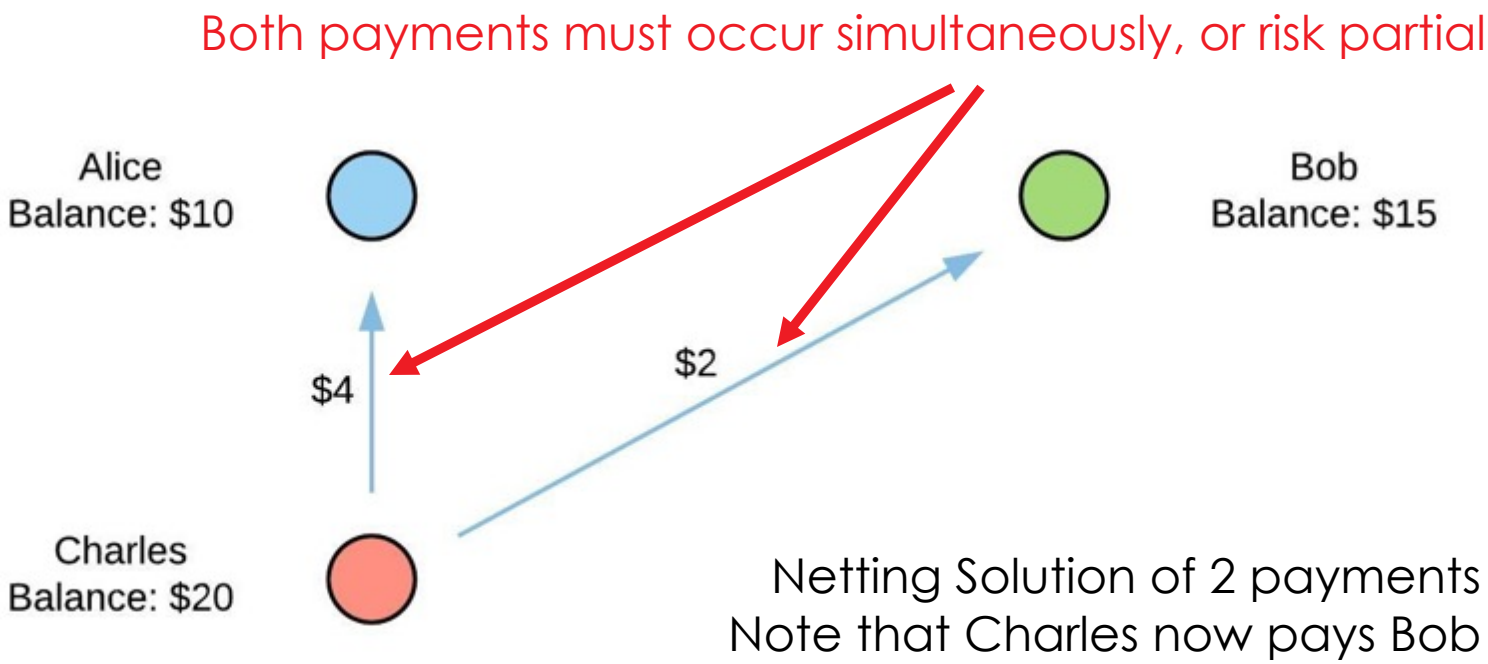
Netting arises where we have cycles of payments. If there's not a cycle then netting doesn't work

A More Tricky Example Resolved

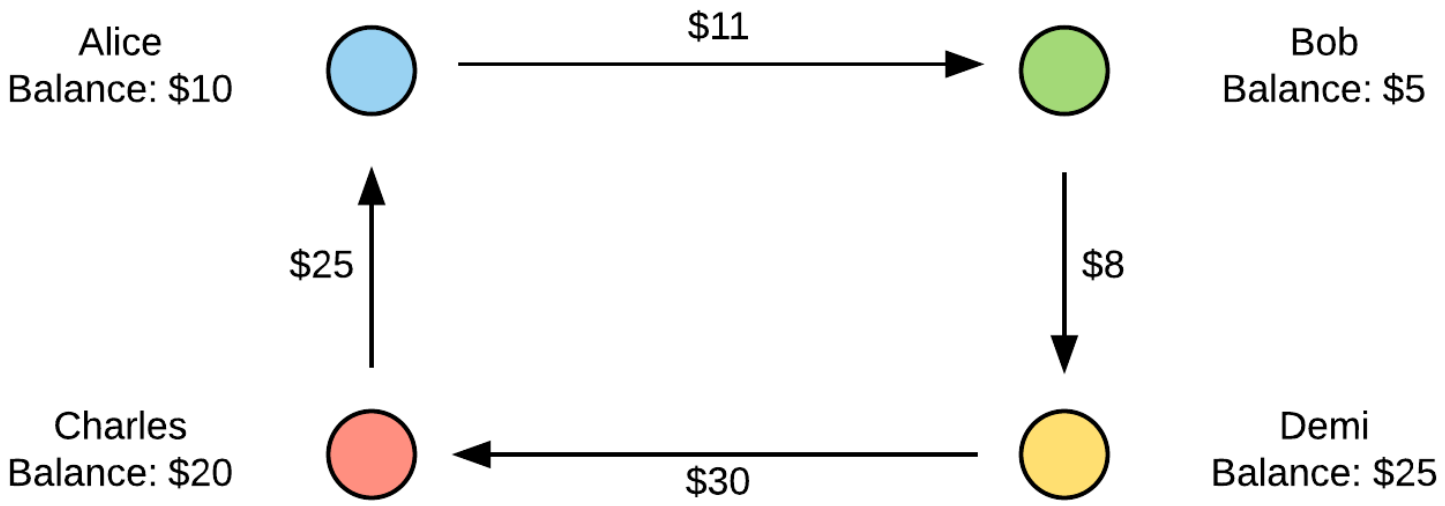


Netting Solution of 2 payments
Note that Charles now pays Bob

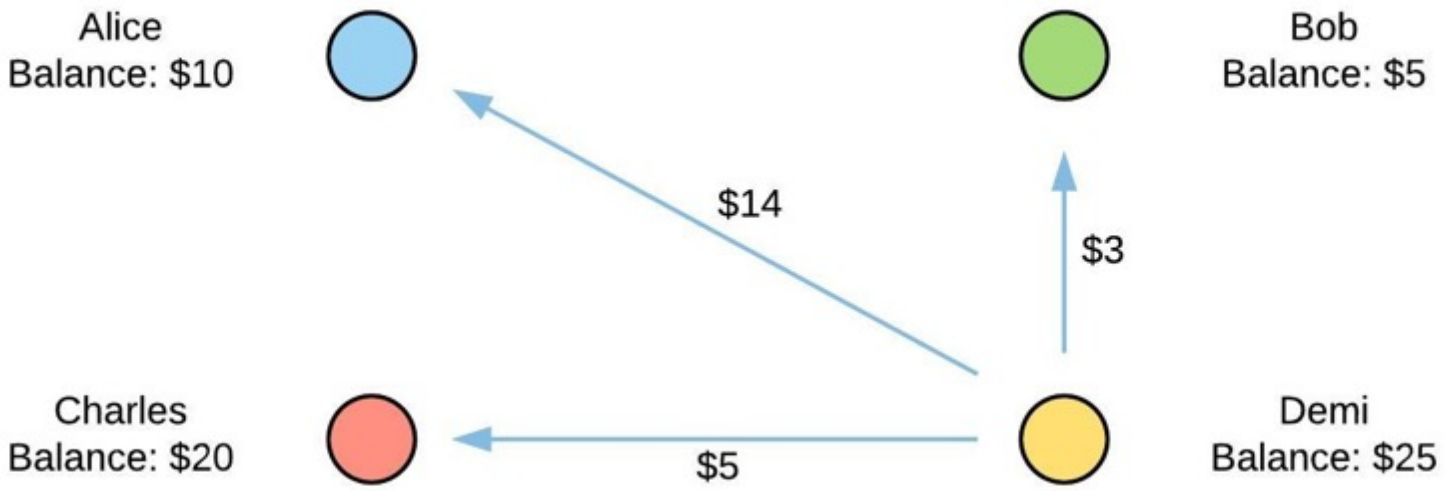
A More Tricky Example Resolved



4 Party Example

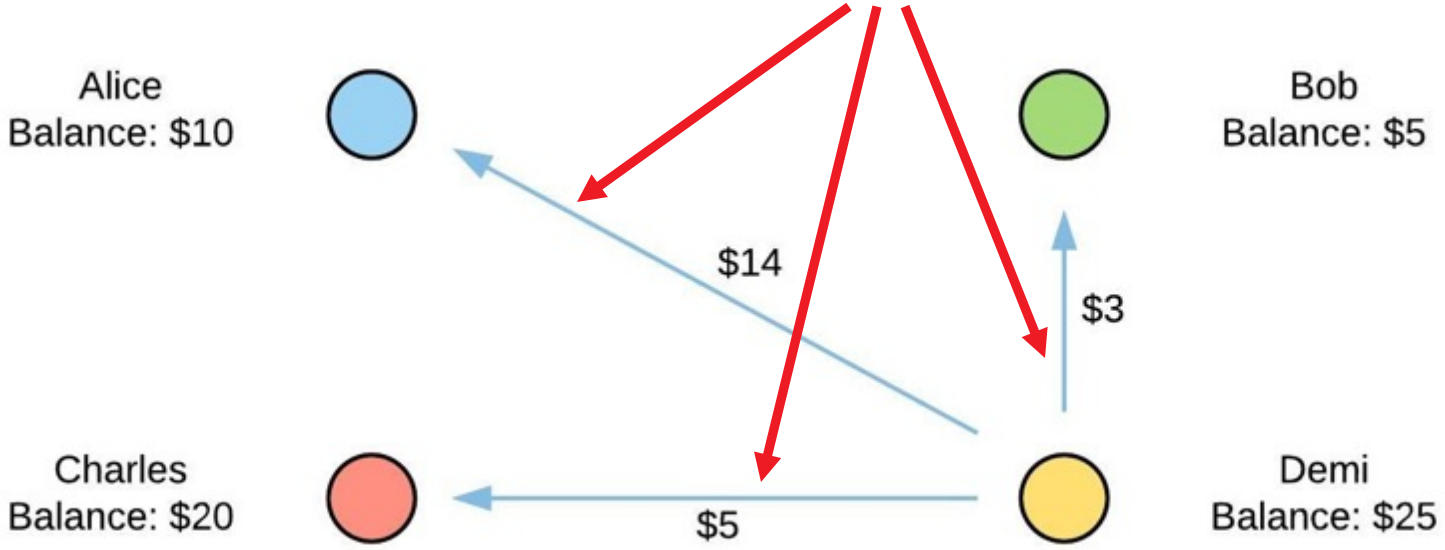


4 Party Example Resolved

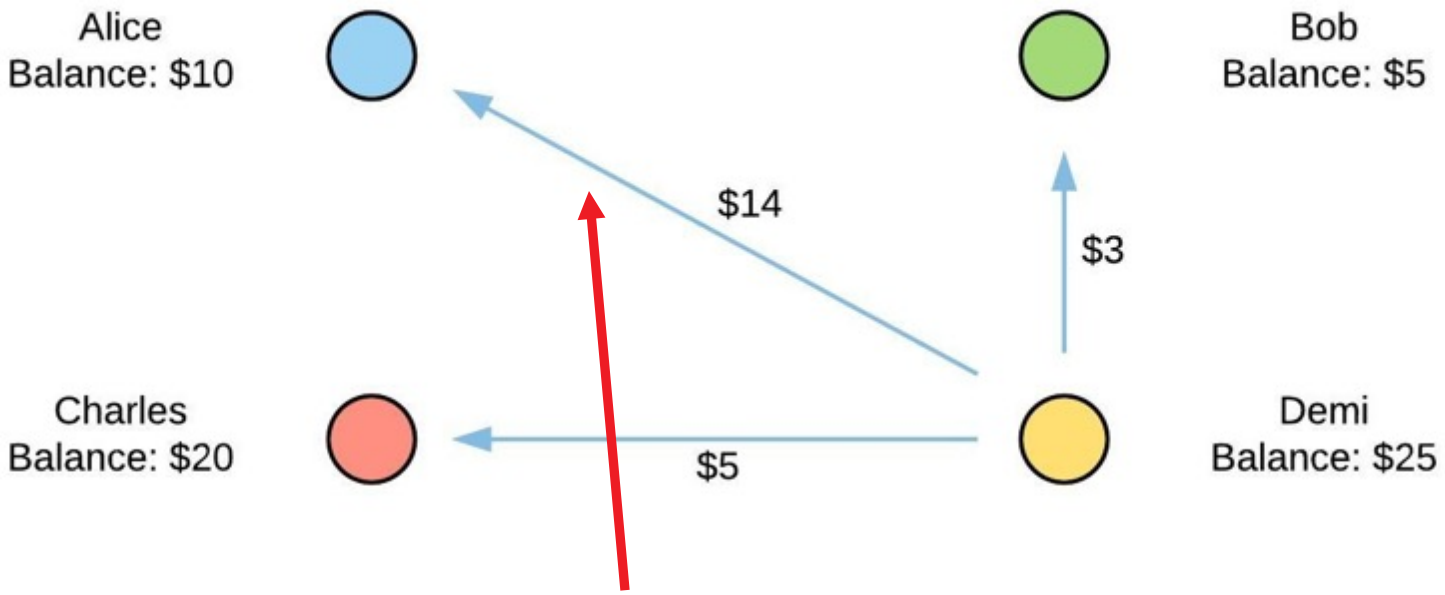


4 Party Example Resolved

All 3 payments must occur simultaneously, or risk partial failure!



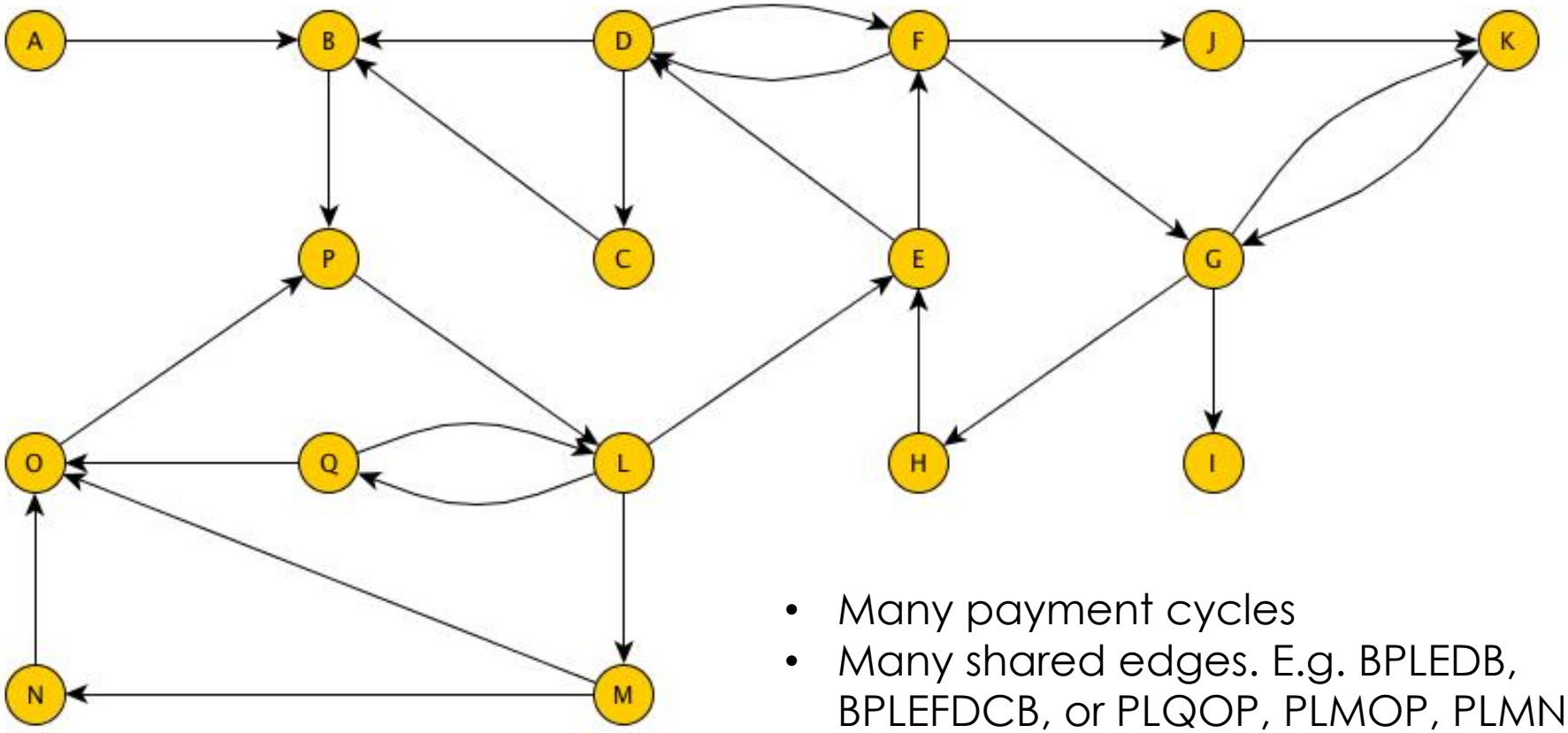
4 Party Example Resolved



Payment from Demi to Alice where there was no existing relationship

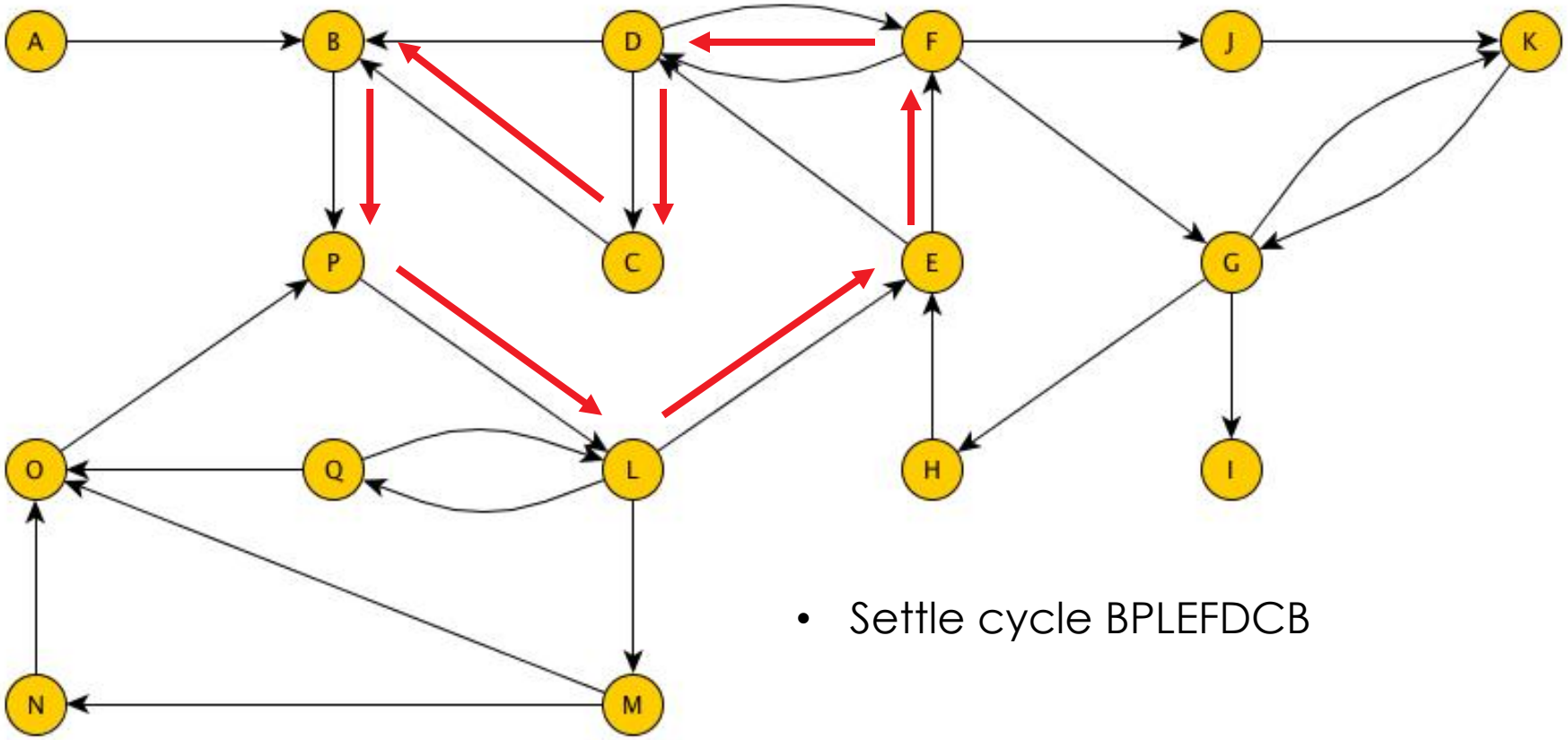
The real world is more complex…

Real World Complexities



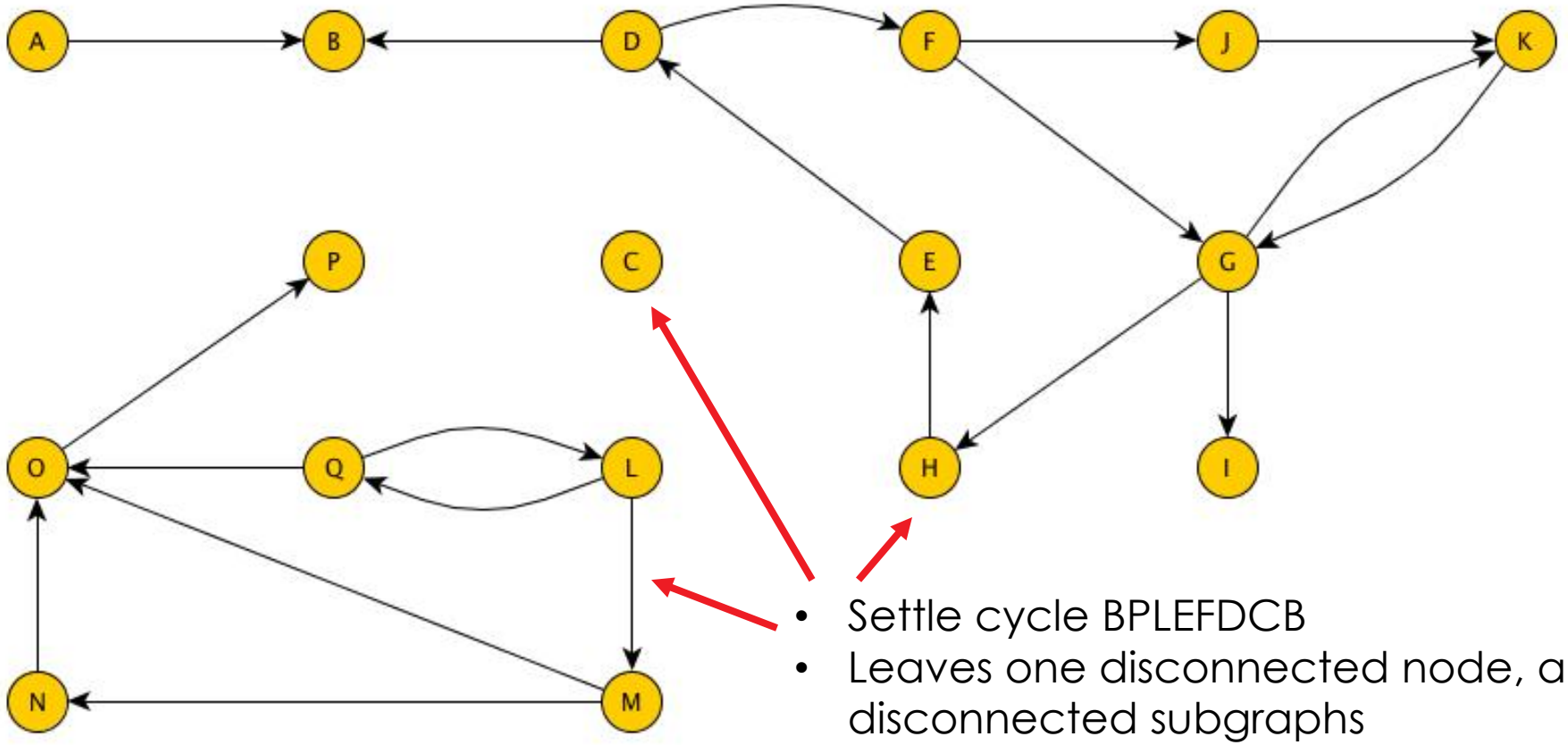
- Many payment cycles
- Many shared edges. E.g. BPLEDB, BPLEFDCB, or PLQOP, PLMOP, PLMNOP
- Graph changes over time

Real World Complexities



- Settle cycle BPLEFDCB

Real World Complexities



- Settle cycle BPLEFDCB
- Leaves one disconnected node, and two disconnected subgraphs

Building this with Corda

Initial Requirements

- Any node may start the netting process
- Trigger may be time-based or needs-based
- Participation is optional
- Each node chooses how much liquidity it will offer towards netting operations

Challenges

- We don’t want to reveal everyone’s unsettled payments (confidential identities)
- We need fast convergence
- We can’t “stop the world”
- No matter what happens, we **must never** be left in an incomplete state!

So why Corda?

Why Corda?

- Corda flows are incredibly powerful building blocks
- Distributed atomic transactions enable solutions to very complex problems

Project Jasper: Domestic Interbank Payments Settlement

Thank you.

Carlos Arena
Director, Business Development
1-917-861-7449
carlos.arena@r3.com
www.r3.com
www.corda.net